Forcepoint DLP API and Service Now Demo Script
Forcepoint DLP API and ServiceNow Demo Script

1. Run the integration script by going to the directory that contains the Python script.

```
(base) jeff.hall@BP-040959 Source Code % ls
EL-DLP_incidents_DIM.json  dlpsync.xlsx
SNOW_incidents.py
(base) jeff.hall@BP-040959 Source Code %
```

2. Modify the payload portion of the script to retrieve the data from the FSM that you want to send to ServiceNow.

   ```python
   payload = json.dumps({
   type: INCIDENT
   from_date: 08/06/2023 18:55:00
   to_date: 10/06/2023 18:55:00
   })
   ```

   Refer to [Forcepoint DLP REST API Guide](#) for full syntax and required fields.

3. Modify the ServiceNow section of the script to connect to your ServiceNow tenet.

   ```python
   service_now_instance = https://dev68380.service-now.com
   service_now_user = admin
   service_now_pass = 'CA9gk-2Vz/Nw'
   def create_service_now_incident(incident):
   # Define the incident data
   data = json.dumps({
   short_description: DLP Incident + str(incident[id])
   description: DLP Incident Details: + json.dumps(incident)
   # add more fields as necessary
   })
   ```
4. Ensure that you have a ServiceNow table created with the following columns.

- id: integer
- severity: string
- action: string
- status: string
- login_name: string
- host_name: string
- task_name: string
- admin_name: string
- update_time: integer
- event_id: integer
- maximum_matches: integer
- transaction_size: integer
- analyzed_by: string
- ignored_incidents: boolean
- event_time: string
- incident_time: string
- channel: string
- policies: string
- partition_index: integer
- destination: string
- detected_by: string
- details: string
- released_incident: boolean
- endpoint_type: string
- classifier_name: string
- number_matches: integer
- policy_name: string
- rule_name: string
5. Once the script has been modified with the correct connection information, execute the script (python SNOW_incidents.py)

6. Once the script is finished, verify that the data has loaded to ServiceNow.

7. As a secondary validation you can execute the viewtable.py script to generate a json file to view the contents of the ServiceNow table.

```
(base) jeff.hall@MBP-640959 Source Code % python viewtable.py
Records saved to records.json successfully.
(base) jeff.hall@MBP-640959 Source Code %
```
About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint’s all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.